§ 310.72 DoD training programs.

(a) To meet these training requirements, establish three general levels of training for those persons who are involved in any way with the design, development, operation, or maintenance of any system of records. These are:

(1) *Orientation.* Training that provides basic understanding of this Regulation as it applies to the individual's job performance. This training shall be provided to personnel, as appropriate, and should be a prerequisite to all other levels of training.

(2) *Specialized training.* Training that provides information as to the application of specific provisions of this part to specialized areas of job performance. Personnel of particular concern include, but are not limited to personnel specialists, finance officers, special investigators, paperwork managers, and other specialists (reports, forms, records, and related functions), computer systems development personnel, computer systems operations personnel, statisticians dealing with personal data and program evaluations, and anyone responsible for implementing or carrying out functions under this part.

(3) *Management.* Training designed to identify for responsible managers (such as, senior system managers, denial authorities, decision-makers, and the managers of the functions described in § 310.70 of this subpart) considerations that they shall take into account when making management decisions regarding the Defense Privacy Program.

(b) Include Privacy Act training in courses of training when appropriate. Stress individual responsibilities and advise individuals of their rights and responsibilities under this part.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

§ 310.73 Training methodology and procedures.

(a) Each DoD Component is responsible for the development of training procedures and methodology.

(b) The Defense Privacy Office, ODASD(A) will assist the Components in developing these training programs and may develop Privacy training programs for use by all DoD Components.

(c) All training programs shall be coordinated with the Defense Privacy Office, ODASD(A) to avoid duplication and to ensure maximum effectiveness.

§ 310.74 Funding for training.

Each DoD Component shall fund its own Privacy training program.

Subpart I—Reports

§ 310.80 Requirements for reports.

The Defense Privacy Office, ODASD(A) shall establish requirements for DoD Privacy Reports and DoD Components may be required to provide data.

§ 310.81 Suspense for submission of reports.

The suspenses for submission of all reports shall be established by the Defense Privacy Office, ODASD(A).

§ 310.82 Reports control symbol.

Any report established by this subpart in support of the Defense Privacy Program shall be assigned Report Control Symbol DD–COMP(A)1379. Special one-time reporting requirements shall be licensed separately in accordance with DoD Directive 5000.19 ''Policies for the Management and Control of Information Requirements'' and DoD Directive 5000.11, ''Data Elements and Data Codes Standardization Program.''

Subpart J—Inspections

§ 310.90 Privacy Act inspections.

During internal inspections, Component inspectors shall be alert for compliance with this part and for managerial, administrative, and operational problems associated with the implementation of the Defense Privacy Program.

§ 310.91 Inspection reporting.

(a) Document the findings of the inspectors in official reports that are furnished the responsible Component officials. These reports, when appropriate, shall reflect overall assets of the Component Privacy Program inspected, or portion thereof, identify deficiencies,

irregularities, and significant problems. Also document remedial actions taken to correct problems identified.

(b) Retain inspections reports and later follow-up reports in accordance with established records disposition standards. These reports shall be made available to the Privacy Program officials concerned upon request.

Subpart K—Privacy Act Enforcement Actions

§ 310.100 Administrative remedies.

Any individual who feels he or she has a legitimate complaint or grievance against the Department of Defense or any DoD employee concerning any right granted by this part shall be permitted to seek relief through appropriate administrative channels.

§ 310.101 Civil actions.

An individual may file a civil suit against a DoD Component or its employees if the individual feels certain provisions of the Act have been violated (see 5 U.S.C. 552a(g), of the Privacy Act.

§ 310.102 Civil remedies.

In addition to specific remedial actions, subsection (g) of the Privacy Act (5 U.S.C. 552a) provides for the payment of damages, court cost, and attorney fees in some cases.

§ 310.103 Criminal penalties.

(a) The Act also provides for criminal penalties (see 5 U.S.C. 552a(i). Any official or employee may be found guilty of a misdemeanor and fined not more than $5,000 if he or she willfully:

(1) Discloses personal information to anyone not entitled to receive the information (see subpart E); or

(2) Maintains a system of records without publishing the required public notice in the FEDERAL REGISTER (see subpart G).

(b) A person who requests or obtains access to any record concerning another individual under false pretenses may be found guilty of misdemeanor and fined up to $5,000.

§ 310.104 Litigation status sheet.

Whenever a complaint citing the Privacy Act is filed in a U.S. District Court against the Department of Defense, a DoD Component, or any DoD employee, the responsible system manager shall notify promptly the Defense Privacy Office, ODASD(A). The litigation status sheet at appendix H provides a standard format for this notification. The initial litigation status sheet forwarded shall, as a minimum, provide the information required by items 1 through 6. A revised litigation status sheet shall be provided at each stage of the litigation. When a court renders a formal opinion or judgment, copies of the judgment and opinion shall be provided to the Defense Privacy Office with the litigation status sheet reporting that judgment or opinion.

Subpart L—Matching Program Procedures

§ 310.110 OMB matching guidelines.

The OMB has issued special guidelines to be followed in programs that match the personal records in the computerized data bases of two or more federal agencies by computer (see appendix I). These guidelines are intended to strike a balance between the interest of the government in maintaining the integrity of federal programs and the need to protect individual privacy expectations. They do not authorize matching programs as such and each matching program must be justified individually in accordance with the OMB guidelines.

§ 310.111 Requesting matching programs.

(a) Forward all requests for matching programs to include necessary routine use amendments (see § 310.62(i) of subpart G) and analysis and proposed matching program reports (see subsection E.6. of appendix I) to the Defense Privacy Office, ODASD(A).

(b) The Defense Privacy Office shall review each request and supporting material and forward the report and system notice amendments to the FEDERAL REGISTER, OMB, and Congress, as appropriate.